手続補正書

（法第１１条の規定による補正）

特 許 庁 長 官 殿

１．国際出願の表示　　ＰＣＴ／ＪＰ９８／００３４２

２．出願人

名　称　トヨタ自動車株式会社

TOYOTA JIDOSHA KABUSHIKI KAISHA

あて名　〒471-0826　日本国愛知県豊田市トヨタ町１番地

1, Toyota-cho, Toyota-shi, Aichi-ken 471-0826, JAPAN

国　籍　日本国　JAPAN

住　所　日本国　JAPAN

３．代理人

氏　名　　７９０４　弁理士　　中　島　　淳

NAKAJIMA Jun

あて名　　〒160-0022　日本国東京都新宿区新宿４丁目３番１７号

ＨＫ新宿ビル７階

太陽国際特許事務所

ＴＡＩＹＯ,　ＮＡＫＡＪＩＭＡ　＆　ＫＡＴＯ

Seventh Floor, HK-Shinjuku Bldg., 3-17,

Shinjuku 4-chome, Shinjuku-ku, Tokyo 160-0022, JAPAN

４．補正の対象　　明細書及び請求の範囲

５．補正の内容

（１）請求の範囲の請求項１、請求項２、請求項３、請求項４、請求項５、請求項６及び請求項７を削除する。

（２）明細書第１頁第３行目、第７行目、第２頁第２６行目、第２８行目の「車載用通信装置及び路車間通信装置」を『路車間通信装置』に改める。

（３）明細書第３頁第３行目から第７頁第１２行目の「上記目的・・・という効果がある。」を以下の如く改める。その結果、差し替え用紙第３頁から第７頁に差し替えられる。

『上記目的を達成するために本発明の路車間通信装置は、路側に設置され、車載用通信手段との間で相互に情報通信する路側通信手段と、第１の電子鍵で送信情報を暗号化すると共に受信情報を復号化する第１の暗号手段とを備えた路側制御手段と、車両及びユーザの少なくとも一方に関係するユーザ情報を記憶すると共に車載用通信手段との間で相互に情報授受する情報授受手段と、第２の電子鍵で出力情報を暗号化すると共に入力情報を復号化する第２の暗号手段とを備えた情報制御手段と、車両側に設置され、前記路側通信装置と相互に情報通信しかつ前記情報制御手段との間で相互に情報授受する車載用通信手段と、前記情報通信のとき第１の電子鍵で送信情報を暗号化しかつ受信情報を復号化すると共に、前記情報授受のとき第２の電子鍵で出力情報を暗号化しかつ入力情報を復号化する第３の暗号手段とを備えた車載用制御手段と、を備えている。

なお、前記第１の暗号手段と路側通信手段、前記第２の暗号手段と情報授受手段、及び前記第３の暗号手段と車載用通信手段の各々は同一基板上に設けることができる。

本発明では、路側制御手段の路側通信手段と車載用制御手段の車載用通信手段との間で相互に情報通信する。また、車載用制御手段の車載用通信手段と情報制御手段の情報授受手段との間で相互に情報授受する。

情報通信のときは、路側制御手段では第１の暗号手段により第１の電子鍵で車載用制御手段へ送信する送信情報を暗号化すると共に車載用制御手段からの受信情報を復号化する。また、車載用制御手段では第３の暗号手段により第１の電子鍵で路側制御手段へ送信する送信情報を暗号化しかつ路側制御手段からの受信情報を復号化する。従って、路側制御手段と車載用制御手段との間で第１の電子鍵を用いて情報を暗号化して相互に情報通信できるので、秘匿性を有させることに

より安全性が保たれる。

情報授受のときは、車載用制御手段では第３の暗号手段により第２の電子鍵で出力情報を暗号化しかつ入力情報を復号化する。情報授受手段は、車両及びユーザの少なくとも一方に関係するユーザ情報を記憶しており、このユーザ情報を車載用制御手段へ出力するとき出力情報として第２の暗号手段により第２の電子鍵で暗号化しかつ車載用制御手段からの入力情報を復号化する。従って、車載用制御手段と情報授受手段との間で第２の電子鍵を用いて情報を暗号化して相互に情報授受できるので、秘匿性を有させることにより安全性が保たれる。

このように、情報通信及び情報授受に異なる電子鍵を用いて独立した秘匿性を有させているので、路車間通信装置として安全性を向上できる。また、独立した秘匿性を有させているので、秘匿性が明らかになるまでを最小限に抑えることができる。

前記第１の暗号手段乃至第３の暗号手段は、秘匿性を有させるもとであるので、これらの暗号手段を明らかにすれば、秘匿性を明らかにできる。そこで、前記第１の暗号手段と路側通信手段、前記第２の暗号手段と情報授受手段、及び前記第３の暗号手段と車載用通信手段の各々を同一基板上、例えば同一チップ上に設けることによって、解析等の解読が困難となり、路車間通信装置の安全性を向上できる。

本発明の路車間通信装置によれば、異なる電子鍵を用いて独立した秘匿性を有させているので、路車間通信装置の安全性を向上できる、という効果がある。

また、第１の暗号手段乃至第３の暗号手段の各々を、対応する路側通信手段、情報授受手段及び車載用通信手段の各々と同一基板上に設けることによって、解析等の解読が困難となり、路車間通信装置の安全性を向上できる、という効果がある。』

（４）明細書第１４頁第２０行目の「車載機３０とのの間」を『車載機３０との間』に改める。

６．添付書類の目録

（１）請求の範囲を別紙の通り補正する。第３０頁は欠頁となる。

（２）明細書の第１頁、第２頁、第３頁、第４頁、第５頁、第６頁、第７頁、及び第１４頁

以上

明細書

路車間通信装置

技術分野

本発明は、路車間通信装置にかかり、特に、車両に搭載された車載用通信装置、及びこの車載用通信装置と路側に設置された路上機との間で通信処理する路車間通信装置に関する。

背景技術

近年、有料施設の利用料金の収受、例えば、有料道路の通行料金の収受等に、料金前納方式または料金後納方式のカードを利用した自動料金収受装置が開発されている。この自動料金収受装置では、有料道路の入口ゲートや出口ゲートで料金収受を自動的に行うため、車両に対して情報を問い合わせるための質問器としてのアンテナを有する路車間通信用路上機（以下、路上機という）を道路側に配設すると共に、問い合わせのあった情報に対する応答をするための応答器としてのアンテナを有する路車間通信用車載機（以下、車載機という）を車両に搭載し、車載機と路上機との間で無線通信により情報の授受を行っている。

車載機と路上機との間で情報を授受するためには、料金情報や車両に関連する車両情報、そしてユーザに関連する情報を記憶する必要がある。このため、大量のデータを記憶できるＩＣカードに情報を書き込ませて用いることもある。

ところで、上記のように、車載機と路上機との間で情報を授受する場合やＩＣカードに対する情報の授受をする場合、情報がその形態のままで用いられるので、ユーザーの意図しない者が情報の内容を容易に明らかにすることができるという問題がある。

そこで、送信された固有コード等の秘密コードが予め定めた複数の秘密コードと一致することを識別して秘匿性を有させることにより安全性を向上させる電子

識別システムが提案されている（特表平６－５１１０９７号公報参照）。

しかしながら、従来の電子識別システムでは、ユーザーに秘密コードを１種類のみ割り当てているため、多数のユーザーを識別するためにはユーザー数に応じた秘密コードを設定しなければならない。このため、多数のユーザーに対して情報の授受を行う路車間通信装置においては装置の負荷が増大する。また、ユーザーに対する秘密コードは１種類のみであるため、その秘密コードが漏洩したときには、ユーザーが使用するシステム、すなわち路車間通信装置の安全性は低下する。

また、車載機と路上機との間で情報を授受することにより自動料金収受するためには、車両に関連する車両情報、そして課金処理のための料金残高等のユーザ個人に関連するユーザ情報を記憶する必要がある。このため、大量のデータを記憶できるＩＣカードに情報を書き込ませて用いることもある。

ところが、上記情報を授受する場合、情報を一般的な記述形態のままで用いると、ユーザーや情報提供者の意図しない者が情報の内容を不法に改ざんや偽造し、不正利用することができるという問題がある。

そこで、路上機と車載機との間で通信される情報を暗号化することにより安全性を向上させる自動料金収集システムが提案されている（特表平６－６０２３７号公報参照）。この技術では、ＩＣカードに記憶された暗号化情報や路上機からの暗号化情報を車載機内で平文化（一般的な記述形態に）し、料金残高等のユーザ情報に対する処理を行っている。

しかしながら、従来の自動料金収集システムでは、車載機内で平文化したユーザ情報を一時的に記憶しているため、料金残高等のユーザ個人に関連するユーザ情報等をユーザーや情報提供者の意図しない者が情報の内容を容易に改ざんすることができ、安全性が低下することがある。

本発明は、上記事実を考慮して、簡単な構成でかつ容易に安全性を向上することができる路車間通信装置を得ることが目的である。

また、上記目的に加え、簡単な構成でかつ情報漏洩や改ざんを困難にして情報通信が可能な路車間通信装置を得ることを目的とする。

発明の開示

上記目的を達成するために

本発明の路車間通信装置は、路側に設置され、車載用通信手段との間で相互に情報通信する路側通信手段と、第１の電子鍵で送信情報を暗号化すると共に受信情報を復号化する第１の暗号手段とを備えた路側制御手段と、車両及びユーザの少なくとも一方に関係するユーザ情報を記憶すると共に車載用通信手段との間で相互に情報授受する情報授受手段と、第２の電子鍵で出力情報を暗号化すると共に入力情報を復号化する第２の暗号手段とを備えた情報制御手段と、車両側に設置され、前記路側通信装置と相互に情報通信しかつ前記情報制御手段との間で相互に情報授受する車載用通信手段と、前記情報通信のとき第１の電子鍵で送信情報を暗号化しかつ受信情報を復号化すると共に、前記情報授受のとき第２の電子鍵で出力情報を暗号化しかつ入力情報を復号化する第３の暗号手段とを備えた車載用制御手段と、を備えている。

なお、前記第１の暗号手段と路側通信手段、前記第２の暗号手段と情報授受手段、及び前記第３の暗号手段と車載用通信手段の各々は同一基板上に設けることができる。

本発明では、路側制御手段の路側通信手段と車載用制御手段の

車載用通信手段との間で相互に情報通信する。また、車載用制御手段の車載用通信手段と情報制御手段の情報授受手段との間で相互に情報授受する。

情報通信のときは、路側制御手段では第１の暗号手段により第１の電子鍵で車載用制御手段へ送信する送信情報を暗号化すると共に車載用制御手段からの受信情報を復号化する。また、車載用制御手段では第３の暗号手段により第１の電子鍵で路側制御手段へ送信する送信情報を暗号化しかつ路側制御手段からの受信情報を復号化する。従って、路側制御手段と車載用制御手段との間で第１の電子鍵を用いて情報を暗号化して相互に情報通信できるので、秘匿性を有させることにより安全性が保たれる。

情報授受のときは、車載用制御手段では第３の暗号手段により第２の電子鍵で出力情報を暗号化しかつ入力情報を復号化する。情報授受手段は、車両及びユーザの少なくとも一方に関係するユーザ情報を記憶しており、このユーザ情報を車載用制御手段へ出力するとき出力情報として第２の暗号手段により第２の電子鍵で暗号化しかつ車載用制御手段からの入力情報を復号化する。従って、車載用制御手段と情報授受手段との間で第２の電子鍵を用いて情報を暗号化して相互に情報授受できるので、秘匿性を有させることにより安全性が保たれる。

このように、情報通信及び情報授受に異なる電子鍵を用いて独立した秘匿性を有させているので、路車間通信装置として安全性を向上できる。また、独立した秘匿性を有させているので、秘匿性が明らかになるまでを最小限に抑えることができる。

前記第１の暗号手段乃至第３の暗号手段は、秘匿性を有させるもとであるので、これらの暗号手段を明らかにすれば、秘匿性を明らかにできる。そこで、前記第１の暗号手段と路側通信手段、前記第２の暗号手段と情報授受手段、及び前記第３の暗号手段と車載用通信手段の各々を同一基板上、例えば同一チップ上に設けることによって、解析等の解読が困難となり、路車間通信装置の安全性を向上できる。

本発明の路車間通信装置によれば、異なる電子鍵を用いて独立した秘匿性を有させているので、路車間通信装置の安全性を向上できる、という効果がある。

また、第１の暗号手段乃至第３の暗号手段の各々を、対応する路側通信手段、情報授受手段及び車載用通信手段の各々と同一基板上に設けることによって、解析等の解読が困難となり、路車間通信装置の安全性を向上できる、という効果がある。

図面の簡単な説明

図１は、本発明の第１実施の形態にかかる自動料金収受システムを示すブロック図である。

図２は、第１実施の形態の自動料金収受システムの途中経路を示す概略斜視図である。

図３は、第１実施の形態の車載機を示すブロック図である。

図４は、第１実施の形態の路上機の一例を示すブロック図である。

図５は、第１実施の形態のＩＣカードの構成を示すブロック図である。

図６は、第１実施の形態の車載機の処理の流れを示すフローチャートである。

図７は、第１実施の形態の途中経路における路上機の処理の流れを示すフローチャートである。

図８は、第１実施の形態の車載機の出口ゲート処理の流れを示すフローチャートである。

図９は、第１実施の形態の出口ゲートの路上機における処理の流れを示すフロ

には、路上機、車載機、及びＩＣカードの各々においてなされる主要な処理、及び各々の間で相互に授受する情報の流れを示した。

図７に示すように、途中経路に設置された路上機では、車載機３０からの応答信号を受信するまでステップ１１４で問合せ信号を送信し、応答信号を受信すると（ステップ１１６で肯定判断）、次のステップ１１８でゲート情報、この場合経路情報を電子鍵Ａで暗号化し（図１１の処理Ｓ１に相当）、次のステップ１２０で暗号化した経路情報等を含む信号を送信する（図１１の授受ｗ１に相当）。上記問合せ信号には路上機のゲート種類を表す情報が含まれている。ゲート種類を表す情報には、例えば、平文化されたゲート番号や「入口」や「途中経路」等の単純な平文情報がある。

なお、入口ゲートの路上機では、上記処理と略同様の処理を行うが、経路情報等を含む信号に代えて入口ゲートを表す入口ゲート番号等を含む信号を暗号化して送信する。また、出口ゲートの路上機でも上記処理と略同様の処理を行うが、通信により行う料金収受処理については後述する。

また、路上機は、ゲート種類を表す情報として単純な平文情報を車載機に送信することを可能としているが、他の情報においても、路上機において単純な平文情報として平文化してもよい情報と、暗号化情報として暗号化すべき情報とを予め区別して選択的に平文情報または暗号化情報にしてもよい。

このように、路上機１０は車載機３０へ向けて暗号化した暗号化情報を送信するので、路上機１０と車載機３０との間で授受される情報は秘匿性を有することが可能となり、情報傍受に対する安全性が向上される。

図６は、車載機の通信処理の詳細を示すもので、ステップ１０２で路上機から問合せ信号を受信するまで待機し、問合せ信号を受信すると（ステップ１０２で肯定判断）、次のステップ１０４で車両情報（自車を特定する識別コード等のＩＤコード等）を読み取ると共に、車両情報を含む信号を応答信号として送信する。

次に、ステップ１０６において路上機からの信号を受信するまで待機し、信号を受信した（ステップ１０６で肯定判断）ときには、路上機と車載機との認証が完了したとして、次のステップ１０８において、問合せ信号に含まれた路上機の

請求の範囲

1．（削除）

2．（削除）

3．（削除）

4．（削除）

5．（削除）

6．（削除）

7．（削除）

8．　路側に設置され、車載用通信手段との間で相互に情報通信する路側通信手段と、第１の電子鍵で送信情報を暗号化すると共に受信情報を復号化する第１の暗号手段とを備えた路側制御手段と、

車両及びユーザの少なくとも一方に関係するユーザ情報を記憶すると共に車載用通信手段との間で相互に情報授受する情報授受手段と、第２の電子鍵で出力情報を暗号化すると共に入力情報を復号化する第２の暗号手段とを備えた情報制御手段と、

車両側に設置され、前記路側通信装置と相互に情報通信しかつ前記情報制御手段との間で相互に情報授受する車載用通信手段と、前記情報通信のとき第１の電子鍵で送信情報を暗号化しかつ受信情報を復号化すると共に、前記情報授受のとき第２の電子鍵で出力情報を暗号化しかつ入力情報を復号化する第３の暗号手段とを備えた車載用制御手段と、

を備えた路車間通信装置。

9．　前記第１の暗号手段と路側通信手段、前記第２の暗号手段と情報授受手段、及び前記第３の暗号手段と車載用通信手段の各々を同一基板上に設けたことを特徴とする請求項８に記載の路車間通信装置。

Amendment Under Article 34

5. Contents of Amendment

(1) Claims 1, 2, 3, 4, 5, 6, and 7 have been canceled.

(2) Page 1, lines 2 to 3 and 6 to 8, page 4, lines 16 to 18 and 21 to 22 of the specification, "(a) vehicle-mounted communication device and (a) road-to-vehicle communication device" has been amended to "(a) road-to-vehicle communication device".

(3) page 5, line 2 through page 14, line 14 of the specification, "In order to achieve the above-described objects, ... of the road-to-vehicle communication device." has been amended as follows. As a result, substituted sheets of pages 1 through 9 have been replaced and pages 1 through 14 have been omitted.

"In order to achieve the above-described objects, a road-to-vehicle communication device of the present invention comprises; a road-to-vehicle communication device comprising: road-side control means being located at a road side, including road-side communication means provided for intercommunication of information with vehicle-mounted communication means, and also including first encryption means for encrypting transmitted information and decoding received information, with a first electronic key; information control means including information transfer means which stores therein user information regarding at least one of a vehicle and a user and through which information is mutually transferred with respect to the vehicle-

mounted communication means, and also including second encryption means for encrypting output information and decoding input information, with a second electronic key; and vehicle-mounted control means being installed on a vehicle side, including vehicle-mounted communication means provided for intercommunication of information with respect to the road-side communication device and for mutual transfer of information with respect to said information control means, and also including third encryption means which, during the communication of information, encrypts transmitted information and decodes received information with the first electronic key, and which during the transfer of information, encrypts output information and decodes input information with the second electronic key.

Meanwhile, each group of a road-to-vehicle communication device according to claim 8, wherein each group of said first encryption means and the road-side communication means, said second encryption means and the information transfer means, and said third encryption means and the vehicle-mounted communication means are provided on the same substrate.

Further, according to the present invention, information is mutually communicated between the road-side communication means of the road-side control means and the vehicle-mounted communication means of the vehicle-mounted

control means. Further, information is mutually transferred between the vehicle-mounted communication means of the vehicle-mounted control means and the information transfer means of the information control means.

During the communication of information, the road-side control means uses the first encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the vehicle-mounted control means and to decode received information from the vehicle-mounted control means. Further, the vehicle-mounted control means uses the third encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the road-side control means and to decode received information from the road-side control means. Accordingly, information can be encrypted using the first electronic key so as to be mutually communicated between the road-side control means and the vehicle-mounted control means, and therefore, the secrecy of information is maintained and the security thereof is thereby protected.

During the transfer of information, the vehicle-mounted control means uses the third encryption means, with the second electronic key, to encrypt output information and to decode input information. The information transfer means stores therein user information regarding at least one of a vehicle and a user. When the user information is outputted to the vehicle-mounted control

means, the information transfer means uses the second encryption means, with the second electronic key, to encrypt, as output information, the user information and to decode input information from the vehicle-mounted control means. Accordingly, information can be encrypted using the second electronic key so as to be mutually transferred between the vehicle-mounted control means and the information transfer means, and therefore, the secrecy is maintained and the security is thereby protected.

As described above, secrecy is independently held using different electronic keys respectively for the communication of information and for the transfer of information, and therefore, the security in the road-to-vehicle communication device can be improved. Further, since secrecy is independently held, leakage of information can be restrained to the minimum until the secrecy becomes clear.

The above-described first, second, and third encryption means are each that which maintains secrecy, and therefore, so long as these encryption means are each made clear, the secrecy can be made clear. Accordingly, by providing each group of the first encryption means and the road-side communication means, the second encryption means and the information transfer means, and the third encryption means and the vehicle-mounted communication means on the same substrate, on the same chip, for example, decoding such as analysis becomes difficult and the

security of the road-to-vehicle communication device can be improved.

In the road-to-vehicle communication device of the present invention, secrecy is independently held using different electronic keys, and therefore, there is an effect wherein the security of the road-to-vehicle communication device can be improved.

Further, by providing the first, second, and third encryption means, respectively together with corresponding road-side communication means, information transfer means, and vehicle-mounted communication means, on the same substrate, there is an effect wherein decoding such as analysis becomes difficult, improving the security of the road-to-vehicle communication device."

(4) Page 14, line 20 of the Japanese specification, two Japanese characters "no-no" has been amended to "no".

6. List of Appended Documents

(1) Claims have been amended as per attached sheets. Pages59 and 60 have been omitted.

(2) Pages through 9 of the specification

SPECIFICATION

ROAD-TO-VEHICLE COMMUNICATION DEVICE

TECHNICAL FIELD

The present invention relates to a road-to-vehicle communication device, and particularly to a vehicle-mounted communication device mounted on a vehicle and to a road-to-vehicle communication device which effects communication processing between the vehicle-mounted communication device and an on-road apparatus installed on a road side.

BACKGROUND ART

In recent years, an automatic toll collecting system has been developed which utilizes a toll pre-paid type card or a toll post-payment type card to receive charges for using charged facilities, for example, to receive a toll charged on a toll road. In the automatic toll collecting system, on-road apparatuses for road-to-vehicle communications (hereinafter referred to as "on-road apparatuses") with antennas, each of which serves as an interrogator for making inquiries with respect to a vehicle for information in order to collect tolls automatically at entrance and exit gates of the toll road, are provided on the road side, and each of vehicle-mounted apparatuses for road-to-vehicle communications (hereinafter referred to as "vehicle-mounted apparatuses") with antennas, each of which serves as a responder for responding to the

information, with respect to which an inquiry was made is mounted on the vehicle, whereby the information is transferred by radio communications between the vehicle-mounted apparatus and the on-road apparatus.

In order to transfer the information between the vehicle-mounted apparatus and the on-road apparatus, toll information or vehicle information about a vehicle, and information about a user must be stored. For this reason, an IC card in which a large quantity of data can be stored may be used with information being written therein.

However, as described above, when the information is transferred between the vehicle-mounted apparatus and the on-road apparatus or when the information is transferred to and received from the IC card, the information is used with a form thereof left unchanged. As a result, there exists a problem that a person not intended by a user can easily disclose contents of the information.

Accordingly, there has been proposed an electronic identification system in which secrecy is kept by identifying that a transmitted secret code such as an inherent code coincides with at least one of a plurality of predetermined secret codes, thereby resulting in improvement of security (see Japanese Patent Publication No. 6-511097).

However, in a conventional electronic identification system, only one kind of secret code is assigned to a user, and

therefore, secret codes must be set correspondingly to the number of users so as to identify a great number of users. For this reason, in a road-to-vehicle communication device in which information is transferred to and received from each of a great number of users, the load on the device increases. Further, only one kind of secret code is assigned to a user, and therefore, when the secret code leaks out, the security of a system used by the user, namely, of the road-to-vehicle communication device, deteriorates.

Further, in order to collect a toll automatically by transferring information between the vehicle-mounted apparatus and the on-road apparatus, vehicle information about a vehicle and user information about a user, such as a balance of charges for accounting must be stored. Accordingly, the IC card in which a large quantity of data can be stored may be used with information being written therein.

However, in a case of transferring the above-described information, when the information is used in a general description form, there exists a problem that a person that is not intended by a user or an information provider can illegally alter or falsify the contents of the information and can also unlawfully utilize such information.

Accordingly, there has been proposed an automatic toll collecting system in which information communicated between an on-road apparatus and a vehicle-mounted apparatus is encoded so as to improve the security (see Japanese Patent Publication No. 6-

60237). In this system, encoded information stored in an IC card or encoded information from the on-road apparatus is made into a common sentence structure (made into a general descriptive form) in the vehicle-mounted apparatus, and processing for user information such as a balance of charges is effected.

However, in the conventional automatic toll collecting system, the user information made into a common sentence structure in the vehicle-mounted apparatus is temporarily stored. Accordingly, a person that is not intended by the user or the information provider can easily falsify the contents of the user information about a user such as the balance of charges, and the like, thereby resulting in deterioration of security.

In view of the above-described circumstances, an object of the present invention is to provide a road-to-vehicle communication device, that can improve security using a simple structure and in a simple manner.

In addition to the above-described object, an object of the present invention is to provide a road-to-vehicle communication device that can allow communication of information using a simple structure by making it difficult to leak or falsify information.

DISCLOSURE OF THE INVENTION

In order to achieve the above-described objects, a road-to-vehicle communication device of the present invention comprises: road-side control means being located at a road side,

including road-side communication means and provided for intercommunication of information with vehicle-mounted communication means, and also including first encryption means for encrypting transmitted information, and decoding received information with a first electronic key; information control means including information transfer means which stores therein user information regarding at least one of a vehicle and a user and through which information is mutually transferred with respect to the vehicle-mounted communication means, and also including second encryption means for encrypting output information, and decoding input information with a second electronic key; and vehicle-mounted control means being installed on a vehicle side, including vehicle-mounted communication means provided for intercommunication of information with respect to the road-side communication device and for mutual transfer of information with respect to the information control means, and also including third encryption means which, during the communication of information, encrypts transmitted information and decodes received information with the first electronic key, and which during the transfer of information, encrypts output information and decodes input information with the second electronic key.

Meanwhile, each group of the first encryption means and the road-side communication means, the second encryption means and the information transfer means, and the third

encryption means and the vehicle-mounted communication means are provided on the same substrate.

Further, according to the present invention, information is mutually communicated between the road-side communication means of the road-side control means and the vehicle-mounted communication means of the vehicle-mounted control means. Further, information is mutually transferred between the vehicle-mounted communication means of the vehicle-mounted control means and the information transfer means of the information control means.

During the communication of information, the road-side control means uses the first encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the vehicle-mounted control means and to decode received information from the vehicle-mounted control means. Further, the vehicle-mounted control means uses the third encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the road-side control means and to decode received information from the road-side control means. Accordingly, information can be encrypted using the first electronic key so as to be mutually communicated between the road-side control means and the vehicle-mounted control means, and therefore, the secrecy of information is maintained and the security thereof is thereby protected.

During the transfer of information, the vehicle-mounted control means uses the third encryption means, with the second electronic key, to encrypt output information and to decode input information. The information transfer means stores therein user information regarding at least one of a vehicle and a user. When the user information is outputted to the vehicle-mounted control means, the information transfer means uses the second encryption means, with the second electronic key, to encrypt, as output information, the user information and to decode input information from the vehicle-mounted control means. Accordingly, information can be encrypted using the second electronic key so as to be mutually transferred between the vehicle-mounted control means and the information transfer means, and therefore, the secrecy is maintained and the security is thereby protected.

As described above, secrecy is independently held using different electronic keys respectively for the communication of information and for the transfer of information, and therefore, the security in the road-to-vehicle communication device can be improved. Further, since secrecy is independently held, leakage of information can be restrained to the minimum until the secrecy becomes clear.

The above-described first, second, and third encryption means are each that which maintains secrecy, and therefore, so long as these encryption means are each made clear, the secrecy

can be made clear. Accordingly, by providing each group of the first encryption means and the road-side communication means, the second encryption means and the information transfer means, and the third encryption means and the vehicle-mounted communication means on the same substrate, on the same chip, for example, decoding such as analysis becomes difficult and the security of the road-to-vehicle communication device can be improved.

In the road-to-vehicle communication device of the present invention, secrecy is independently held using different electronic keys, and therefore, there is an effect wherein the security of the road-to-vehicle communication device can be improved.

Further, by providing the first, second, and third encryption means, respectively together with corresponding road-side communication means, information transfer means, and vehicle-mounted communication means, on the same substrate, there is an effect wherein decoding such as analysis becomes difficult, improving the security of the road-to-vehicle communication device.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram that shows an automatic toll receiving system according to a first embodiment of the present invention.

Fig. 2 is a schematic perspective view that shows a mid-route in the automatic toll receiving system of the first embodiment.

Fig. 3 is a block diagram that shows a vehicle-mounted apparatus of the first embodiment.

WHAT IS CLAIMED IS:

1. (canceled)

2. (canceled)

3. (canceled)

4. (canceled)

5. (canceled)

6. (canceled)

7. (canceled)

8. A road-to-vehicle communication device comprising:

road-side control means being located at a road side, including road-side communication means provided for intercommunication of information with vehicle-mounted communication means, and also including first encryption means for encrypting transmitted information and decoding received information, with a first electronic key;

information control means including information transfer means which stores therein user information regarding at least one of a vehicle and a user and through which information is mutually transferred with respect to the vehicle-mounted communication means, and also including second encryption means for encrypting output information and decoding input information, with a second electronic key; and

vehicle-mounted control means being installed on a vehicle side, including vehicle-mounted communication means provided for intercommunication of information with respect to

the road-side communication device and for mutual transfer of information with respect to said information control means, and also including third encryption means which, during the communication of information, encrypts transmitted information and decodes received information with the first electronic key, and which during the transfer of information, encrypts output information and decodes input information with the second electronic key.

9. A road-to-vehicle communication device according to claim 8, wherein each group of said first encryption means and the road-side communication means, said second encryption means and the information transfer means, and said third encryption means and the vehicle-mounted communication means are provided on the same substrate.

Amendment Under Article 34

5. Contents of Amendment

(1) Claims 1, 2, 3, 4, 5, 6, and 7 have been canceled.

(2) Page 1, lines 2 to 3 and 6 to 8, page 4, lines 16 to 18 and 21 to 22 of the specification, "(a) vehicle-mounted communication device and (a) road-to-vehicle communication device" has been amended to "(a) road-to-vehicle communication device".

(3) page 5, line 2 through page 14, line 14 of the specification, "In order to achieve the above-described objects, ... of the road-to-vehicle communication device." has been amended as follows. As a result, substituted sheets of pages 1 through 9 have been replaced and pages 1 through 14 have been omitted.

"In order to achieve the above-described objects, a road-to-vehicle communication device of the present invention comprises; a road-to-vehicle communication device comprising: road-side control means being located at a road side, including road-side communication means provided for intercommunication of information with vehicle-mounted communication means, and also including first encryption means for encrypting transmitted information and decoding received information, with a first electronic key; information control means including information transfer means which stores therein user information regarding at least one of a vehicle and a user and through which information is mutually transferred with respect to the vehicle-

mounted communication means, and also including second encryption means for encrypting output information and decoding input information, with a second electronic key; and vehicle-mounted control means being installed on a vehicle side, including vehicle-mounted communication means provided for intercommunication of information with respect to the road-side communication device and for mutual transfer of information with respect to said information control means, and also including third encryption means which, during the communication of information, encrypts transmitted information and decodes received information with the first electronic key, and which during the transfer of information, encrypts output information and decodes input information with the second electronic key.

Meanwhile, each group of a road-to-vehicle communication device according to claim 8, wherein each group of said first encryption means and the road-side communication means, said second encryption means and the information transfer means, and said third encryption means and the vehicle-mounted communication means are provided on the same substrate.

Further, according to the present invention, information is mutually communicated between the road-side communication means of the road-side control means and the vehicle-mounted communication means of the vehicle-mounted

control means. Further, information is mutually transferred between the vehicle-mounted communication means of the vehicle-mounted control means and the information transfer means of the information control means.

During the communication of information, the road-side control means uses the first encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the vehicle-mounted control means and to decode received information from the vehicle-mounted control means. Further, the vehicle-mounted control means uses the third encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the road-side control means and to decode received information from the road-side control means. Accordingly, information can be encrypted using the first electronic key so as to be mutually communicated between the road-side control means and the vehicle-mounted control means, and therefore, the secrecy of information is maintained and the security thereof is thereby protected.

During the transfer of information, the vehicle-mounted control means uses the third encryption means, with the second electronic key, to encrypt output information and to decode input information. The information transfer means stores therein user information regarding at least one of a vehicle and a user. When the user information is outputted to the vehicle-mounted control

means, the information transfer means uses the second encryption means, with the second electronic key, to encrypt, as output information, the user information and to decode input information from the vehicle-mounted control means. Accordingly, information can be encrypted using the second electronic key so as to be mutually transferred between the vehicle-mounted control means and the information transfer means, and therefore, the secrecy is maintained and the security is thereby protected.

As described above, secrecy is independently held using different electronic keys respectively for the communication of information and for the transfer of information, and therefore, the security in the road-to-vehicle communication device can be improved. Further, since secrecy is independently held, leakage of information can be restrained to the minimum until the secrecy becomes clear.

The above-described first, second, and third encryption means are each that which maintains secrecy, and therefore, so long as these encryption means are each made clear, the secrecy can be made clear. Accordingly, by providing each group of the first encryption means and the road-side communication means, the second encryption means and the information transfer means, and the third encryption means and the vehicle-mounted communication means on the same substrate, on the same chip, for example, decoding such as analysis becomes difficult and the

security of the road-to-vehicle communication device can be improved.

In the road-to-vehicle communication device of the present invention, secrecy is independently held using different electronic keys, and therefore, there is an effect wherein the security of the road-to-vehicle communication device can be improved.

Further, by providing the first, second, and third encryption means, respectively together with corresponding road-side communication means, information transfer means, and vehicle-mounted communication means, on the same substrate, there is an effect wherein decoding such as analysis becomes difficult, improving the security of the road-to-vehicle communication device."

(4) Page 14, line 20 of the Japanese specification, two Japanese characters "no-no" has been amended to "no".

6. List of Appended Documents

(1) Claims have been amended as per attached sheets. Pages59 and 60 have been omitted.

(2) Pages through 9 of the specification

SPECIFICATION

ROAD-TO-VEHICLE COMMUNICATION DEVICE

TECHNICAL FIELD

The present invention relates to a road-to-vehicle communication device, and particularly to a vehicle-mounted communication device mounted on a vehicle and to a road-to-vehicle communication device which effects communication processing between the vehicle-mounted communication device and an on-road apparatus installed on a road side.

BACKGROUND ART

In recent years, an automatic toll collecting system has been developed which utilizes a toll pre-paid type card or a toll post-payment type card to receive charges for using charged facilities, for example, to receive a toll charged on a toll road. In the automatic toll collecting system, on-road apparatuses for road-to-vehicle communications (hereinafter referred to as "on-road apparatuses") with antennas, each of which serves as an interrogator for making inquiries with respect to a vehicle for information in order to collect tolls automatically at entrance and exit gates of the toll road, are provided on the road side, and each of vehicle-mounted apparatuses for road-to-vehicle communications (hereinafter referred to as "vehicle-mounted apparatuses") with antennas, each of which serves as a responder for responding to the

information, with respect to which an inquiry was made is mounted on the vehicle, whereby the information is transferred by radio communications between the vehicle-mounted apparatus and the on-road apparatus.

In order to transfer the information between the vehicle-mounted apparatus and the on-road apparatus, toll information or vehicle information about a vehicle, and information about a user must be stored. For this reason, an IC card in which a large quantity of data can be stored may be used with information being written therein.

However, as described above, when the information is transferred between the vehicle-mounted apparatus and the on-road apparatus or when the information is transferred to and received from the IC card, the information is used with a form thereof left unchanged. As a result, there exists a problem that a person not intended by a user can easily disclose contents of the information.

Accordingly, there has been proposed an electronic identification system in which secrecy is kept by identifying that a transmitted secret code such as an inherent code coincides with at least one of a plurality of predetermined secret codes, thereby resulting in improvement of security (see Japanese Patent Publication No. 6-511097).

However, in a conventional electronic identification system, only one kind of secret code is assigned to a user, and

therefore, secret codes must be set correspondingly to the number of users so as to identify a great number of users. For this reason, in a road-to-vehicle communication device in which information is transferred to and received from each of a great number of users, the load on the device increases. Further, only one kind of secret code is assigned to a user, and therefore, when the secret code leaks out, the security of a system used by the user, namely, of the road-to-vehicle communication device, deteriorates.

Further, in order to collect a toll automatically by transferring information between the vehicle-mounted apparatus and the on-road apparatus, vehicle information about a vehicle and user information about a user, such as a balance of charges for accounting must be stored. Accordingly, the IC card in which a large quantity of data can be stored may be used with information being written therein.

However, in a case of transferring the above-described information, when the information is used in a general description form, there exists a problem that a person that is not intended by a user or an information provider can illegally alter or falsify the contents of the information and can also unlawfully utilize such information.

Accordingly, there has been proposed an automatic toll collecting system in which information communicated between an on-road apparatus and a vehicle-mounted apparatus is encoded so as to improve the security (see Japanese Patent Publication No. 6-

60237). In this system, encoded information stored in an IC card or encoded information from the on-road apparatus is made into a common sentence structure (made into a general descriptive form) in the vehicle-mounted apparatus, and processing for user information such as a balance of charges is effected.

However, in the conventional automatic toll collecting system, the user information made into a common sentence structure in the vehicle-mounted apparatus is temporarily stored. Accordingly, a person that is not intended by the user or the information provider can easily falsify the contents of the user information about a user such as the balance of charges, and the like, thereby resulting in deterioration of security.

In view of the above-described circumstances, an object of the present invention is to provide a road-to-vehicle communication device, that can improve security using a simple structure and in a simple manner.

In addition to the above-described object, an object of the present invention is to provide a road-to-vehicle communication device that can allow communication of information using a simple structure by making it difficult to leak or falsify information.

DISCLOSURE OF THE INVENTION

In order to achieve the above-described objects, a road-to-vehicle communication device of the present invention comprises: road-side control means being located at a road side,

including road-side communication means and provided for intercommunication of information with vehicle-mounted communication means, and also including first encryption means for encrypting transmitted information, and decoding received information with a first electronic key; information control means including information transfer means which stores therein user information regarding at least one of a vehicle and a user and through which information is mutually transferred with respect to the vehicle-mounted communication means, and also including second encryption means for encrypting output information, and decoding input information with a second electronic key; and vehicle-mounted control means being installed on a vehicle side, including vehicle-mounted communication means provided for intercommunication of information with respect to the road-side communication device and for mutual transfer of information with respect to the information control means, and also including third encryption means which, during the communication of information, encrypts transmitted information and decodes received information with the first electronic key, and which during the transfer of information, encrypts output information and decodes input information with the second electronic key.

Meanwhile, each group of the first encryption means and the road-side communication means, the second encryption means and the information transfer means, and the third

encryption means and the vehicle-mounted communication means are provided on the same substrate.

Further, according to the present invention, information is mutually communicated between the road-side communication means of the road-side control means and the vehicle-mounted communication means of the vehicle-mounted control means. Further, information is mutually transferred between the vehicle-mounted communication means of the vehicle-mounted control means and the information transfer means of the information control means.

During the communication of information, the road-side control means uses the first encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the vehicle-mounted control means and to decode received information from the vehicle-mounted control means. Further, the vehicle-mounted control means uses the third encryption means, with the first electronic key, to encrypt transmitted information to be transmitted to the road-side control means and to decode received information from the road-side control means. Accordingly, information can be encrypted using the first electronic key so as to be mutually communicated between the road-side control means and the vehicle-mounted control means, and therefore, the secrecy of information is maintained and the security thereof is thereby protected.

During the transfer of information, the vehicle-mounted control means uses the third encryption means, with the second electronic key, to encrypt output information and to decode input information. The information transfer means stores therein user information regarding at least one of a vehicle and a user. When the user information is outputted to the vehicle-mounted control means, the information transfer means uses the second encryption means, with the second electronic key, to encrypt, as output information, the user information and to decode input information from the vehicle-mounted control means. Accordingly, information can be encrypted using the second electronic key so as to be mutually transferred between the vehicle-mounted control means and the information transfer means, and therefore, the secrecy is maintained and the security is thereby protected.

As described above, secrecy is independently held using different electronic keys respectively for the communication of information and for the transfer of information, and therefore, the security in the road-to-vehicle communication device can be improved. Further, since secrecy is independently held, leakage of information can be restrained to the minimum until the secrecy becomes clear.

The above-described first, second, and third encryption means are each that which maintains secrecy, and therefore, so long as these encryption means are each made clear, the secrecy

can be made clear. Accordingly, by providing each group of the first encryption means and the road-side communication means, the second encryption means and the information transfer means, and the third encryption means and the vehicle-mounted communication means on the same substrate, on the same chip, for example, decoding such as analysis becomes difficult and the security of the road-to-vehicle communication device can be improved.

In the road-to-vehicle communication device of the present invention, secrecy is independently held using different electronic keys, and therefore, there is an effect wherein the security of the road-to-vehicle communication device can be improved.

Further, by providing the first, second, and third encryption means, respectively together with corresponding road-side communication means, information transfer means, and vehicle-mounted communication means, on the same substrate, there is an effect wherein decoding such as analysis becomes difficult, improving the security of the road-to-vehicle communication device.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram that shows an automatic toll receiving system according to a first embodiment of the present invention.

Fig. 2 is a schematic perspective view that shows a mid-route in the automatic toll receiving system of the first embodiment.

Fig. 3 is a block diagram that shows a vehicle-mounted apparatus of the first embodiment.

WHAT IS CLAIMED IS:

1. (canceled)

2. (canceled)

3. (canceled)

4. (canceled)

5. (canceled)

6. (canceled)

7. (canceled)

8. A road-to-vehicle communication device comprising:

road-side control means being located at a road side, including road-side communication means provided for intercommunication of information with vehicle-mounted communication means, and also including first encryption means for encrypting transmitted information and decoding received information, with a first electronic key;

information control means including information transfer means which stores therein user information regarding at least one of a vehicle and a user and through which information is mutually transferred with respect to the vehicle-mounted communication means, and also including second encryption means for encrypting output information and decoding input information, with a second electronic key; and

vehicle-mounted control means being installed on a vehicle side, including vehicle-mounted communication means provided for intercommunication of information with respect to

the road-side communication device and for mutual transfer of information with respect to said information control means, and also including third encryption means which, during the communication of information, encrypts transmitted information and decodes received information with the first electronic key, and which during the transfer of information, encrypts output information and decodes input information with the second electronic key.

9. A road-to-vehicle communication device according to claim 8, wherein each group of said first encryption means and the road-side communication means, said second encryption means and the information transfer means, and said third encryption means and the vehicle-mounted communication means are provided on the same substrate.